

Requested Patent: EP0860882A2
Title: ANTI-TAMPER BOND WIRE SHIELD FOR AN INTEGRATED CIRCUIT ;
Abstracted Patent: EP0860882 ;
Publication Date: 1998-08-26 ;
Inventor(s): CANDELORE BRANT (US) ;
Applicant(s): GEN INSTRUMENT CORP (US) ;
Application Number: EP19980103099 19980221 ;
Priority Number(s): US19970804792 19970224 ;
IPC Classification: H01L23/58; G11C7/00; G06F1/00; G06F12/14 ;
Equivalents: CA2230065, CN1200570, JP10294325, TW388942, US5861662 ;

ABSTRACT:

An anti-tamper shield for an integrated circuit (IC) includes a bond wire which passes through a protective layer such as an epoxy encapsulating layer of the IC. The bond wire carries a signal, such as a steady state current, which allows an active component of the IC, such as a secure processor, to function. The bond wire is carried within and/or proximate to the encapsulating layer such that a decapsulation of the IC will cause a rupture of the electrically conductive member, thereby rendering the processor non-functional. The bond wire may be coupled to the processor in a variety of configurations, including the use of internal or external bond pads, lead frame contacts, and/or directly to a computer board on which the IC is carried. A metallic shield layer may be located between the active component and a top portion of the encapsulating layer to prevent a pirate from using an electron microscope, for example, to survey the active component region.

(19)



Europäisches Patentamt

European Patent Office

Office européen des brevets



(11) EP 0 860 882 A2

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:
26.08.1998 Bulletin 1998/35

(51) Int. Cl.⁶: H01L 23/58, G11C 7/00,
G06F 1/00, G06F 12/14

(21) Application number: 98103099.2

(22) Date of filing: 21.02.1998

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC
NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 24.02.1997 US 804792

(71) Applicant:
General Instrument Corporation
Horsham, Pennsylvania 19044 (US)

(72) Inventor: Candelore, Brant
San Diego, California 92109 (US)

(74) Representative:
Hoeger, Stellrecht & Partner
Uhlandstrasse 14 c
70182 Stuttgart (DE)

(54) Anti-tamper bond wire shield for an integrated circuit

(57) An anti-tamper shield for an integrated circuit (IC) includes a bond wire which passes through a protective layer such as an epoxy encapsulating layer of the IC. The bond wire carries a signal, such as a steady state current, which allows an active component of the IC, such as a secure processor, to function. The bond wire is carried within and/or proximate to the encapsulating layer such that a decapsulation of the IC will cause a rupture of the electrically conductive member, thereby rendering the processor non-functional. The bond wire may be coupled to the processor in a variety of configurations, including the use of internal or external bond pads, lead frame contacts, and/or directly to a computer board on which the IC is carried. A metallic shield layer may be located between the active component and a top portion of the encapsulating layer to prevent a pirate from using an electron microscope, for example, to survey the active component region.

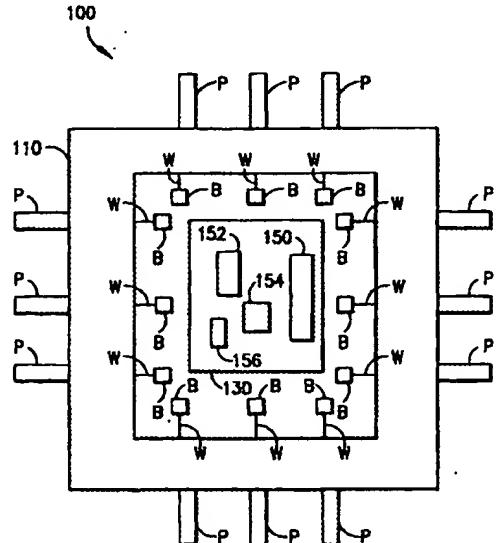


FIG.1

EP 0 860 882 A2

Description**BACKGROUND OF THE INVENTION**

The present invention relates to the protection of integrated circuits (ICs), and more particularly, to a scheme for preventing the reverse engineering of ICs. The invention is particularly useful in protecting secure ICs which are used in cable and satellite television decoders to prevent unauthorized users from receiving television broadcasts. The invention is equally useful in protecting secure ICs used in other applications, including terminals and smart cards for electronic funds transactions, premises access control, electronic games, and the like.

Due to the continuing popularity of the pay television market, there exists a tremendous financial motivation for unauthorized persons known as "pirates" to modify the access control of set-top boxes (e.g., decoders) to allow the reception of television programming without payment of the required subscription fees. The modified decoders are purchased by unscrupulous individuals through various markets and used to illegally receive and view the television signals.

To produce a modified decoder, a pirate must extract certain information from a genuine decoder which is usually known only to the authorized manufacturer. The decoder typically includes a secure (e.g., cryptographic) processor which contains information such as cryptographic keys which are used in descrambling a scrambled television signal or other programming service signal (e.g., audio or data). Since the secure processor performs access control functions, it is a focal point of the pirate's attention. Accordingly, the pirate will employ various techniques in an attempt to gain information from the secure processor.

One common attack technique is known as "probing." A secure processor includes an integrated circuit (IC) which is fabricated as a monolithic device with an ensemble of active and passive components, including transistors, resistors, capacitors, and diodes which are interconnected within a monolithic block of semiconductor material. During probing, ICs such as very large scale integrated (VLSI) circuits are subject to an invasive attack wherein the die (e.g., IC or "chip") is exposed by decapsulation. During decapsulation, the compound material which encapsulates or surrounds the die is systematically removed. Then, probes which measure current and other parameters are used to monitor the electronic signals in the active components of the chip. The term "tampering" as used herein is meant to encompass both probing and decapsulation.

A pirate may perform the following decapsulation steps to prepare a chip for probing. First, the chip is removed from the decoder board, with the die still inside the IC package. Generally, this is the case when a chip is mounted on a large board. The decoder board may be a computer board such as those used in a personal

computer (PC). If the chip requires a direct current from a battery or the like to circumvent a self-destruct feature, then battery wires are soldered to a positive voltage pin (e.g., V_{batt}) pin and to a negative voltage pin (e.g., V_{ss}) on the outside of the chip prior to removal from the board. The chip is then removed from the board with the battery wires still attached. If the battery power is interrupted, the chip may self-destruct by erasing critical information stored in memory. The pirate can identify the appropriate battery pins by taking resistance measurements of the traces on the board which are connected to the battery, and then confirming by taking voltage readings of the traces with a main voltage (e.g., V_{cc}) off.

Second, the location of the die within the encapsulating compound of the IC package can be determined by taking an x-ray of the IC package. Third, a mechanical grinder can be used to remove as much of the encapsulating compound as possible above the top surface of the die without damaging the die. Fourth, chemical etching or plasma etching is performed to remove the last portions of encapsulating compound which remain over the area of the die which is to be probed. Some chemical etchants work so well on the encapsulating compound that the grinding step can often be skipped.

In current chip designs, including those for application specific ICs (ASICs), a pirate will generally not encounter significant obstacles in performing the four steps above. Removal of the chip from the board with the battery wires still attached is usually considered to be the most delicate operation. Thus, the undamaged die, which is protected by an inert glassivation coating, can be exposed by a pirate as long as a short circuit or open circuit of the battery power is not created. Furthermore, damage to bond wires can also easily be avoided. Bond wires may connect bond pads of the chip to package pads in the protective encapsulating package, and are located on the periphery of the device, as will be discussed in greater detail below. The decapsulation process can avoid exposing the die in the area where critical bond pads are located, that is, where the battery power is input into the active component.

One approach to deterring probing is discussed in commonly-assigned U.S. Patent 4,933,898, issued June 12, 1990 to Gilberg et al., entitled "Secure Integrated Circuit Chip With Conductive Shield." Gilberg et al. disclose using one or more conductive layers to overlay a secure area of an IC. The conductive layers shield the secure area from inspection and carry a power signal to the IC. Removal of one of the layers by a pirate causes the loss of power to the components of the secure area. However, the implementation of this approach is somewhat complex.

Accordingly, it would be desirable to provide an apparatus which deters or otherwise hinders probing of an IC chip by a pirate. In particular, it would be desirable to provide a barrier to decapsulation which uses stand-

ard bond wires to render the IC non-functional when the bond wire is ruptured. The barrier should be compatible with existing chip designs and inexpensive to implement. The present invention provides a system having the above and other advantages.

SUMMARY OF THE INVENTION

In accordance with the present invention, an anti-tamper shield for an integrated circuit (IC) is presented. The shield is adapted for use with an IC which includes a substrate for carrying an active component, such as a secure processor which may include a memory, CPU, and other micro-electronic components. The IC may have a protective layer such as an epoxy encapsulating layer for protecting the processor.

The anti-tamper shield comprises an electrically conductive member such as a bond wire for carrying a signal which allows the processor to function. This signal may include a steady state electrical current which is supplied by a battery via positive and negative terminals. The wire may be carried, at least in part, in a protective layer of the IC such that removal of the protective layer will rupture the wire, thereby causing an open circuit.

The wire may be coupled to the processor in a variety of configurations. For example, the wire may be coupled between a first terminus which is external to the processor and a second terminus which is internal to the processor. Furthermore, the electrically conductive member may extend between points which are external and/or internal to the micro-electronic circuits of the processor. The terminus may be a bond pad within the processor, or a bond pad or lead frame contact outside the processor, for example.

Alternatively, the wire or other electrically conductive member may be coupled between first and second terminuses, both of which are external to the processor. The wire may optionally traverse the top surface of the micro-electronic circuit, and/or may extend in a region away from the micro-electronic circuit and/or processor.

The electrically conductive member may be coupled between first and second terminuses, both of which are internal to the processor.

In another configuration, the electrically conductive member may comprise conductive epoxy, and/or a substance which is tailored to have a desired resistance to an etchant. The conductive epoxy may be printed as a trace over the micro-electronic circuit. In this case, the use of an etchant by a pirate to remove the protective layer of the IC will also destroy the conductive epoxy, thereby terminating the signal which allows the processor to function.

In all configurations, even if a pirate was successful in decapsulating the die with the conductive members intact, the conductive member would pose a physical obstacle to probing with mechanical probes or an electron microscope since a conductive member suspended

in space present a hazard that is difficult to overcome. Probes must be continually lifted and reconfigured into new positions by the pirate to allow different angles of approach in order to probe a die and avoid rupturing any of the conductive members. In fact, the electrically conductive member may be formed in a grid pattern to further aggravate probe positioning.

Furthermore, a metallic shield layer may be disposed between the processor and the top portion of the encapsulating layer to prevent a pirate from using an electron microscope, for example, to survey (i.e., map) the processor or the micro-electronic circuits contained therein. The use of a metallic shield in conjunction with the anti-tamper bond-wire shield poses an additional obstacle to the pirate, thereby making the pirate's task more time-consuming and expensive.

The IC may be carried in a smart card. Moreover, a portion of the body of the smart card may provide the encapsulating layer.

Optionally, a wire which does not carry an electrical signal may extend, at least in part, over the micro-electronic component to deter probing of the micro-electronic component. In particular, the wire may form a grid pattern which makes it difficult for a pirate to position and move a probe tip near the micro-electronic component.

BRIEF DESCRIPTION OF THE DRAWINGS

FIGURE 1 is a simplified diagram illustrating a decapsulated integrated circuit.

FIGURE 2 is a cross-sectional view illustrating an integrated circuit with an anti-tamper bond wire shield in accordance with the present invention.

FIGURE 3 is a top view of a secure processor of an integrated circuit with an anti-tamper bond wire shield in accordance with the present invention.

FIGURE 4 is a top view of a secure processor of an integrated circuit with an anti-probing wire grid shield in accordance with the present invention.

DETAILED DESCRIPTION OF THE INVENTION

An anti-tamper apparatus for an integrated circuit (IC) is presented for preventing active components, such as a secure processor used in a television decoder, from being tampered with (e.g., reversed engineered).

FIGURE 1 is a simplified diagram of a decapsulated integrated circuit. The integrated circuit (IC), shown generally at 100, includes an epoxy encapsulating compound region 110. A number of package pins P are connected to respective bond pads B via lead wires W. A bond pad or die pad is one of many metal connection pins that reside in the periphery of the die 130, and are used to couple a unique circuit portion (e.g., input/output (I/O) port) with a corresponding external package pin. The pad pitch is the distance (e.g., in microns)

between the midpoints of the adjacent I/O bond pads B. The die can comprise, for example, a silicon micro-chip which contains micro-electronic devices. The package pins P, wires W and bond pads B carry current to and from the IC 100, and are exposed when the epoxy compound which normally covers the die 130 is removed using the decapsulating steps discussed previously.

Wirebond is a step in the die packaging process where thin wires are bonded between the die I/O pads and the package pads. The die 130 includes exemplary active components 150, 152, 154 and 156. In particular, component 150 may be a secure processor which includes cryptographic information. Thus, the die components are exposed and can be probed by a pirate to ascertain the cryptographic information and other operating characteristics of the active components.

FIGURE 2 is a cross-sectional view of an integrated circuit with an anti-tamper bond wire shield in accordance with the present invention. The IC, shown generally at 200, includes a top epoxy layer 210 and a bottom epoxy layer 212. An electrically conductive member such as a bond wire 270 is shown coupling bond pads 260 and 262. Note that the electrically conductive member need not have a circular cross-section. Thus, it should be understood that the terms "electrically conductive member" and "wire" as used herein are not limited to a single filament member having a circular cross-section, but may encompass configurations including a number of filaments which are wound or twisted together, a configuration with a varying cross section, a configuration with a rectangular cross section, a mesh configuration, a configuration wherein a single wire is coupled to more than two terminals, or virtually any electrically conductive member. In particular, the wires may be provided in a grid pattern with a spacing which is small enough to prevent a probe from passing through the mesh or moving easily within the mesh, as discussed below in conjunction with FIGURE 4. In fact, a grid configuration may be used even when the wire does not carry an electrical signal which the processor requires to function. The mere presence of the grid serves as a deterrent to probing.

Furthermore, the electrically conductive member 270 may comprise a substance such as conductive epoxy which is formed by doping epoxy with a conductive material such as silver to achieve a desired conductivity. Advantageously, the epoxy can be selected to have a resistance to etching which is similar to the resistance of the protective layer of the IC, and/or the resistance of the conductive epoxy can be tailored according to a specific etchant which a pirate is expected to use. The conductive epoxy may be printed directly to the surface of the die.

A glassivation layer 220 is also provided. Glassivation refers to an inert protective coating which is placed over the entire surface of a completed die to protect the circuit. Glassivation protects the surface of the die from chemical and moisture contamination, handling dam-

age, and the possibility of shorting the die caused by loose particles. It can also inhibit metal migration and other metal degradation.

5 A shield 230 is a metal layer that provides current to various components within the IC 200, such as the components 150-156 of FIGURE 1. If power to the shield is interrupted, then a secure processing component may self-destruct such that cryptographic data which is stored in the secure processor is erased. Additionally, 10 the shield 230 serves to prevent a pirate from using a scanning electron microscope to detect changes (e.g., voltage changes) in portions of the secure processor, such as a random access memory (RAM), and blurs the distinction between parts which are coated by the shield. The shield may be located within the encapsulating layer, which includes one or more protective layers which are disposed above the chip in the substrate 250. A passivation layer 240 is a protective surface coat comprising, for example, silicon dioxide which is deposited over the surface of the die during various diffusion steps. The substrate 250 is the physical material upon which the IC is fabricated or assembled. For a monolithic device, the substrate typically comprises silicon.

15 As discussed, a chip such as an ASIC can be 20 decapsulated by a pirate to expose the die in a relatively straightforward manner even when the die has a battery powered self-destruct feature. In accordance with the present invention, one or more electrically conductive members such as standard bond wires of the type used to connect a bond pad with a package pad, such as bond wire 270, are situated to cover the die such that an anti-tamper shield is formed. In particular, during fabrication of a chip, the encapsulating compound is in a molten state and flows around and below the anti-tamper bond wire which are suspended over the die. 25 When the compound (e.g., layer 210) has solidified, it provides a formidable obstacle as it is more difficult for a pirate to use mechanical grinding equipment to remove the wire-embedded layer for fear of breaking (e.g., rupturing) the bond wires and initiating the self-destruct feature of the secure processor.

30 For example, in the case of a cryptographic chip 35 powered by a direct current from a battery or the like, if the electrically conductive member is ruptured, power to a RAM which maintains the secret data will be cut, thereby causing the data to be erased. If a electrically conductive member is used in a component which did not have a battery powered erasure feature, then the electrically conductive member may instead carry various control signals. However, even the rupturing of such a control signal-carrying electrically conductive member without the erasure of secret data would thwart a pirate's probing attack until the pirate performed the necessary time-consuming and difficult repair.

35 Moreover, even if a pirate could somehow carefully remove the layer 210 without rupturing the electrically conductive member, by the time the epoxy below the conductive member is etched, the conductive member

may be eaten away and ruptured due to the corrosivity of the etchant. This is true since the metal in the conductive member is chosen to react to the chemical etchants which are useful in etching the epoxy. Thus, it may be desirable to choose a material such as aluminum, which has a relatively low resistance to etchants. Other metals, such as gold, have a relatively high resistance to etchants. Moreover, if a conductive member is powered by a battery, etchants will react in a more aggressive way. Generally, the selection of the conductive member material can be tailored to provide a desired resistance to particular etchants. Conductive epoxy is particularly useful as it may be formulated to have a similar resistance to etching as the epoxy encapsulating layer.

FIGURE 3 is a top view illustrating, in simplified form, a secure processor of an integrated circuit with an anti-tamper bond wire shield in accordance with the present invention. The secure processor 150, includes exemplary micro-electronic components such as a RAM 300, a central processing unit (CPU) 302, a read-only memory (ROM) 304, and a Data Encryption Standard (DES) processor 306. However, note that the present invention is equally applicable to non-secure processors which may be protected to preserve unencrypted but proprietary information. Thus, the term "processor" as used herein is meant to encompass encrypted processors, non-encrypted processors, and virtually any type of micro-electronic circuit or micro-electronic component.

FIGURE 3 is meant to show a variety of possible arrangements of conductive members such as bond wires in an anti-tamper shield of an IC. It should be understood that not all of the bond wires shown are required, and that the specific number and positioning of the bond wires can vary.

In one example configuration, a signal having a positive voltage V_{batt} may be supplied to a bond pad 310, which is electrically coupled to a bond pad 312, a trace 314, and a bond pad 316. Similarly, a negative voltage V_{ss} is present at a bond pad 318, which is electrically coupled to a bond pad 320, a trace 322, and a bond pad 324. The voltage V_{batt} may be used to provide a current which, when terminated, triggers an automatic erasure (e.g., self-destruct) feature of the processor 150.

Bond wires can be coupled between bond pads which are external to the processor 150 and bond pads which are internal (e.g., located within) the processor 150. For example, a bond wire 313 may be coupled between the external bond pad 312 and the internal bond pad 326 in the region of the RAM 300. Pad 326 is shown as being located outside the RAM 300, but may couple an electrical signal to the RAM 300 via a trace, for example, not shown.

Similarly, in the region of the CPU 302, a bond wire 319 may be coupled between the bond pad 320 which is external to the processor 150 and the bond pad 328

of the CPU 302 which is internal to the processor 150. A bond wire 317 may be coupled between the bond pad 316 which is external to the processor 150 and the bond pad 332 of the CPU which is internal to the processor 150. In the region of the ROM 304, a bond wire 325 may be coupled between the external bond pad 324 and the internal bond pad 336 of the ROM 304.

Bond wires can also be coupled between bond pads which are both internal to the processor 150. For example, a bond wire 331 may be coupled between internal bond pads 330 and 338.

Bond wires can be further be coupled between bond pads which are external to the processor 150. For example, a bond wire 341 may be coupled between external bond pads 340 and 342, and a bond wire 345 may be coupled between external bond pads 344 and 346.

Additionally, bond wires can be coupled between lead frame contacts and external or internal bond pads, or other lead frame contacts. For example, a bond wire 351 may be coupled between a lead frame contact 350 and an external bond pad 352. A bond wire 356 may be coupled between a lead frame contact 355 and an internal bond pad 357. A bond wire 361 may be coupled between a lead frame contact 360 and another lead frame contact 362. As indicated by the broken line, the lead frame contact 362 may be a package lead which is located further from the processor 150 than the contact 360. Note that the positioning of the lead frame contacts and bond pads in FIGURE 3 is not necessarily to scale. A bond wire 366 may be coupled between a lead frame contact 365 and an external bond pad 367. A bond wire 371 may be coupled between a lead frame contact 370 and another lead frame contact 372.

Furthermore, a bond wire can be coupled between a bond pad or lead frame contact of the processor 150 directly to a decoder board (e.g., personal computer (PC) board) on which the processor 150 is carried, or any other location which allows the bond wire to carry a current loop or other signal for use by the processor 150. In this case, mere removal of the chip package from the board or other location will rupture the anti-tamper bond wire.

Additionally, a bond wire can be coupled between external pads, such as pads 340 and 342, where the bond wire does not extend over the surface of the processor 150, but extends away from the surface of the processor, for example, in a loop (not shown). A similar configuration can be had with the contacts, such as contacts 370 and 372, where the bond wire 371 extends away from the processor 150. Thus, the bond wire can be routed to a region which is somewhat distant from the processor 150, e.g., where the pirate may not expect to find it.

The secure processor 150 may be carried in an IC which is embedded in a smart card. A smart card is typically a plastic credit-card sized device which contains ICs. The smart card is inserted into a reader to allow a

component to interface with the ICs. There are various methods of packaging ICs into a card. For example, after an IC is wire bonded to contacts of a lead frame, epoxy can be transfer molded around the die prior to injection molding of a card. Another approach is to apply epoxy to a cavity in a card body prior to insertion of the contact/die assembly into the same smart card body. In either case, an epoxy encapsulating compound can be made to flow around the conductive members.

Furthermore, the body of the smart card forms part of the encapsulating layer of the IC. Moreover, the bond wires of the IC may be routed in the body of the smart card away from the region in which the IC is embedded such that any tampering with the smart card ruptures the bond wires.

The use of conductive epoxy to provide an anti-tamper shield in a smart card is particularly advantageous since it allows a lower profile for the card. The conductive epoxy can be printed as a thin trace which extends over the IC.

FIGURE 4 is a top view of a secure processor of an integrated circuit with an anti-probing wire grid shield in accordance with the present invention. Bond wires may be provided in a grid pattern with a spacing which is small enough to prevent a probe tip from passing through the mesh or moving easily within the mesh. In fact, this configuration may be used even when the wire does not carry an electrical signal which the processor requires to function. The mere presence of the wires (e.g., dummy wires) in a grid serves as a deterrent to probing.

In an example implementation of a wire grid shield, a processor 450 includes a micro-electronic component 410 such as a memory. Bond wires 421, 423, and 425 are coupled between bond pads 420 and 430, 422 and 432, and 424 and 434, respectively. Similarly, bond wires 451, 453, and 454 are coupled between bond pads 448 and 460, 452 and 462, and 454 and 464, respectively. The wires form a grid pattern, shown generally at 460, which covers the micro-electronic component 410. The dimensions of the grid 460 may be adjusted to aggravate the movement of the tip of a probe which a pirate may use.

The wires of the grid 460 may optionally carry a signal which is used by the micro-electronic circuit 410 to operate. In this case, it may be preferable for some or all of the wires to avoid contacting each other to avoid a short circuit. If so, the wires may be displaced from one another as required to maintain the grid pattern while avoiding a short circuit.

When dummy wires are used in a grid or other pattern, it is desirable to select a wire composition which has a high resistance to the chemical etchants which may be used by a pirate in etching the epoxy or other protective layer of the IC. As mentioned, metals such as gold, for example, have a relatively high resistance to etchants.

Accordingly, it can be seen that there are many pos-

sible configurations for using bond wires in an anti-tamper shield to prevent an unauthorized decapsulation of a chip. With the anti-tamper shield of the present invention, a pirate employing a mechanical grinder for decapsulation would have to leave a great deal of the encapsulating compound in place or risk rupturing the bond wires. In fact, the bond wires can be arranged such that most of the epoxy must be left undisturbed to avoid rupturing the wires. If a wire is ruptured, a self-destruct sequence of the chip may be initiated, or a required control signal path may be terminated, thereby requiring a time-consuming and difficult repair by the pirate.

Moreover, even if the wire does not initiate a self-destruct sequence or carry a required control signal, the mere presence of the wire can interfere with efforts to map the chip via an x-ray machine. Thus, the mere presence of "dummy" bond wires in an anti-tamper shield, particularly in a grid pattern, will serve as a deterrent, as the pirate may not know whether rupturing the wires will render the processor non-functional. In either case, the pirate's task is made much more difficult, time-consuming and expensive, if not impossible.

Although the invention has been described in connection with various specific embodiments, those skilled in the art will appreciate that numerous adaptations and modifications may be made thereto without departing from the spirit and scope of the invention as set forth in the claims. For example, the invention is not limited to use with chips which have an epoxy encapsulating layer, but may be adapted for use with a chip which has virtually any type of protective layer, or even no protective layer. For instance, the invention may be used with a device such as an electrically programmable read-only memory (EPROM), which can be erased when exposed to ultraviolet light. An EPROM is typically protected by an air gap and a transparent window. In this case, the electrically conductive member may be carried simply in the air gap, and will pose an obstacle to a pirate even without the epoxy layer.

Claims

1. An anti-tamper apparatus for protecting an active component of an integrated circuit (IC) from probing, said apparatus comprising:

a wire adapted to carry a signal which allows said active component to function; wherein: said wire extends, at least in part, over said active component to hinder access thereto when said active component is functioning.

2. The apparatus of claim 1, wherein:

said wire extends between first and second terminuses; and
said first terminus is external to said processor

and said second terminus is internal to said processor.

3. The apparatus of claim 1, wherein:
 5
 said wire extends between first and second terminuses; and
 said first and second terminuses are both external to said processor.

4. The apparatus of claim 1, wherein:
 10
 said wire extends between first and second terminuses; and
 said first and second terminuses are both internal to said processor.

5. The apparatus of one of the preceding claims, wherein:
 15
 20
 said wire forms a grid pattern.

6. The apparatus of one of the preceding claims, wherein:
 25
 said wire is carried, at least in part, within a protective layer of said IC such that said wire is adapted to rupture when said protective layer is removed.

7. The apparatus of one of the preceding claims, further comprising:
 30
 35
 a metallic shield layer which shields at least a portion of said active circuit.

8. The apparatus of one of the preceding claims, wherein:
 40
 said IC is embedded in a smart card; and
 said wire is adapted to rupture when said IC is removed from said smart card.

9. An anti-tamper apparatus for protecting an active component of an integrated circuit (IC) from probing, said apparatus comprising:
 45
 50
 a conductive epoxy member adapted to carry a signal which allows said active component to function; wherein:
 55
 said conductive epoxy member extends, at least in part, over said active component to hinder access thereto when said active component is functioning.

10. The apparatus of claim 9, wherein:
 60
 65
 70
 75
 80
 85
 90
 95
 100
 105
 110
 115
 120
 125
 130
 135
 140
 145
 150
 155
 160
 165
 170
 175
 180
 185
 190
 195
 200
 205
 210
 215
 220
 225
 230
 235
 240
 245
 250
 255
 260
 265
 270
 275
 280
 285
 290
 295
 300
 305
 310
 315
 320
 325
 330
 335
 340
 345
 350
 355
 360
 365
 370
 375
 380
 385
 390
 395
 400
 405
 410
 415
 420
 425
 430
 435
 440
 445
 450
 455
 460
 465
 470
 475
 480
 485
 490
 495
 500
 505
 510
 515
 520
 525
 530
 535
 540
 545
 550
 555
 560
 565
 570
 575
 580
 585
 590
 595
 600
 605
 610
 615
 620
 625
 630
 635
 640
 645
 650
 655
 660
 665
 670
 675
 680
 685
 690
 695
 700
 705
 710
 715
 720
 725
 730
 735
 740
 745
 750
 755
 760
 765
 770
 775
 780
 785
 790
 795
 800
 805
 810
 815
 820
 825
 830
 835
 840
 845
 850
 855
 860
 865
 870
 875
 880
 885
 890
 895
 900
 905
 910
 915
 920
 925
 930
 935
 940
 945
 950
 955
 960
 965
 970
 975
 980
 985
 990
 995
 1000
 1005
 1010
 1015
 1020
 1025
 1030
 1035
 1040
 1045
 1050
 1055
 1060
 1065
 1070
 1075
 1080
 1085
 1090
 1095
 1100
 1105
 1110
 1115
 1120
 1125
 1130
 1135
 1140
 1145
 1150
 1155
 1160
 1165
 1170
 1175
 1180
 1185
 1190
 1195
 1200
 1205
 1210
 1215
 1220
 1225
 1230
 1235
 1240
 1245
 1250
 1255
 1260
 1265
 1270
 1275
 1280
 1285
 1290
 1295
 1300
 1305
 1310
 1315
 1320
 1325
 1330
 1335
 1340
 1345
 1350
 1355
 1360
 1365
 1370
 1375
 1380
 1385
 1390
 1395
 1400
 1405
 1410
 1415
 1420
 1425
 1430
 1435
 1440
 1445
 1450
 1455
 1460
 1465
 1470
 1475
 1480
 1485
 1490
 1495
 1500
 1505
 1510
 1515
 1520
 1525
 1530
 1535
 1540
 1545
 1550
 1555
 1560
 1565
 1570
 1575
 1580
 1585
 1590
 1595
 1600
 1605
 1610
 1615
 1620
 1625
 1630
 1635
 1640
 1645
 1650
 1655
 1660
 1665
 1670
 1675
 1680
 1685
 1690
 1695
 1700
 1705
 1710
 1715
 1720
 1725
 1730
 1735
 1740
 1745
 1750
 1755
 1760
 1765
 1770
 1775
 1780
 1785
 1790
 1795
 1800
 1805
 1810
 1815
 1820
 1825
 1830
 1835
 1840
 1845
 1850
 1855
 1860
 1865
 1870
 1875
 1880
 1885
 1890
 1895
 1900
 1905
 1910
 1915
 1920
 1925
 1930
 1935
 1940
 1945
 1950
 1955
 1960
 1965
 1970
 1975
 1980
 1985
 1990
 1995
 2000
 2005
 2010
 2015
 2020
 2025
 2030
 2035
 2040
 2045
 2050
 2055
 2060
 2065
 2070
 2075
 2080
 2085
 2090
 2095
 2100
 2105
 2110
 2115
 2120
 2125
 2130
 2135
 2140
 2145
 2150
 2155
 2160
 2165
 2170
 2175
 2180
 2185
 2190
 2195
 2200
 2205
 2210
 2215
 2220
 2225
 2230
 2235
 2240
 2245
 2250
 2255
 2260
 2265
 2270
 2275
 2280
 2285
 2290
 2295
 2300
 2305
 2310
 2315
 2320
 2325
 2330
 2335
 2340
 2345
 2350
 2355
 2360
 2365
 2370
 2375
 2380
 2385
 2390
 2395
 2400
 2405
 2410
 2415
 2420
 2425
 2430
 2435
 2440
 2445
 2450
 2455
 2460
 2465
 2470
 2475
 2480
 2485
 2490
 2495
 2500
 2505
 2510
 2515
 2520
 2525
 2530
 2535
 2540
 2545
 2550
 2555
 2560
 2565
 2570
 2575
 2580
 2585
 2590
 2595
 2600
 2605
 2610
 2615
 2620
 2625
 2630
 2635
 2640
 2645
 2650
 2655
 2660
 2665
 2670
 2675
 2680
 2685
 2690
 2695
 2700
 2705
 2710
 2715
 2720
 2725
 2730
 2735
 2740
 2745
 2750
 2755
 2760
 2765
 2770
 2775
 2780
 2785
 2790
 2795
 2800
 2805
 2810
 2815
 2820
 2825
 2830
 2835
 2840
 2845
 2850
 2855
 2860
 2865
 2870
 2875
 2880
 2885
 2890
 2895
 2900
 2905
 2910
 2915
 2920
 2925
 2930
 2935
 2940
 2945
 2950
 2955
 2960
 2965
 2970
 2975
 2980
 2985
 2990
 2995
 3000
 3005
 3010
 3015
 3020
 3025
 3030
 3035
 3040
 3045
 3050
 3055
 3060
 3065
 3070
 3075
 3080
 3085
 3090
 3095
 3100
 3105
 3110
 3115
 3120
 3125
 3130
 3135
 3140
 3145
 3150
 3155
 3160
 3165
 3170
 3175
 3180
 3185
 3190
 3195
 3200
 3205
 3210
 3215
 3220
 3225
 3230
 3235
 3240
 3245
 3250
 3255
 3260
 3265
 3270
 3275
 3280
 3285
 3290
 3295
 3300
 3305
 3310
 3315
 3320
 3325
 3330
 3335
 3340
 3345
 3350
 3355
 3360
 3365
 3370
 3375
 3380
 3385
 3390
 3395
 3400
 3405
 3410
 3415
 3420
 3425
 3430
 3435
 3440
 3445
 3450
 3455
 3460
 3465
 3470
 3475
 3480
 3485
 3490
 3495
 3500
 3505
 3510
 3515
 3520
 3525
 3530
 3535
 3540
 3545
 3550
 3555
 3560
 3565
 3570
 3575
 3580
 3585
 3590
 3595
 3600
 3605
 3610
 3615
 3620
 3625
 3630
 3635
 3640
 3645
 3650
 3655
 3660
 3665
 3670
 3675
 3680
 3685
 3690
 3695
 3700
 3705
 3710
 3715
 3720
 3725
 3730
 3735
 3740
 3745
 3750
 3755
 3760
 3765
 3770
 3775
 3780
 3785
 3790
 3795
 3800
 3805
 3810
 3815
 3820
 3825
 3830
 3835
 3840
 3845
 3850
 3855
 3860
 3865
 3870
 3875
 3880
 3885
 3890
 3895
 3900
 3905
 3910
 3915
 3920
 3925
 3930
 3935
 3940
 3945
 3950
 3955
 3960
 3965
 3970
 3975
 3980
 3985
 3990
 3995
 4000
 4005
 4010
 4015
 4020
 4025
 4030
 4035
 4040
 4045
 4050
 4055
 4060
 4065
 4070
 4075
 4080
 4085
 4090
 4095
 4100
 4105
 4110
 4115
 4120
 4125
 4130
 4135
 4140
 4145
 4150
 4155
 4160
 4165
 4170
 4175
 4180
 4185
 4190
 4195
 4200
 4205
 4210
 4215
 4220
 4225
 4230
 4235
 4240
 4245
 4250
 4255
 4260
 4265
 4270
 4275
 4280
 4285
 4290
 4295
 4300
 4305
 4310
 4315
 4320
 4325
 4330
 4335
 4340
 4345
 4350
 4355
 4360
 4365
 4370
 4375
 4380
 4385
 4390
 4395
 4400
 4405
 4410
 4415
 4420
 4425
 4430
 4435
 4440
 4445
 4450
 4455
 4460
 4465
 4470
 4475
 4480
 4485
 4490
 4495
 4500
 4505
 4510
 4515
 4520
 4525
 4530
 4535
 4540
 4545
 4550
 4555
 4560
 4565
 4570
 4575
 4580
 4585
 4590
 4595
 4600
 4605
 4610
 4615
 4620
 4625
 4630
 4635
 4640
 4645
 4650
 4655
 4660
 4665
 4670
 4675
 4680
 4685
 4690
 4695
 4700
 4705
 4710
 4715
 4720
 4725
 4730
 4735
 4740
 4745
 4750
 4755
 4760
 4765
 4770
 4775
 4780
 4785
 4790
 4795
 4800
 4805
 4810
 4815
 4820
 4825
 4830
 4835
 4840
 4845
 4850
 4855
 4860
 4865
 4870
 4875
 4880
 4885
 4890
 4895
 4900
 4905
 4910
 4915
 4920
 4925
 4930
 4935
 4940
 4945
 4950
 4955
 4960
 4965
 4970
 4975
 4980
 4985
 4990
 4995
 5000
 5005
 5010
 5015
 5020
 5025
 5030
 5035
 5040
 5045
 5050
 5055
 5060
 5065
 5070
 5075
 5080
 5085
 5090
 5095
 5100
 5105
 5110
 5115
 5120
 5125
 5130
 5135
 5140
 5145
 5150
 5155
 5160
 5165
 5170
 5175
 5180
 5185
 5190
 5195
 5200
 5205
 5210
 5215
 5220
 5225
 5230
 5235
 5240
 5245
 5250
 5255
 5260
 5265
 5270
 5275
 5280
 5285
 5290
 5295
 5300
 5305
 5310
 5315
 5320
 5325
 5330
 5335
 5340
 5345
 5350
 5355
 5360
 5365
 5370
 5375
 5380
 5385
 5390
 5395
 5400
 5405
 5410
 5415
 5420
 5425
 5430
 5435
 5440
 5445
 5450
 5455
 5460
 5465
 5470
 5475
 5480
 5485
 5490
 5495
 5500
 5505
 5510
 5515
 5520
 5525
 5530
 5535
 5540
 5545
 5550
 5555
 5560
 5565
 5570
 5575
 5580
 5585
 5590
 5595
 5600
 5605
 5610
 5615
 5620
 5625
 5630
 5635
 5640
 5645
 5650
 5655
 5660
 5665
 5670
 5675
 5680
 5685
 5690
 5695
 5700
 5705
 5710
 5715
 5720
 5725
 5730
 5735
 5740
 5745
 5750
 5755
 5760
 5765
 5770
 5775
 5780
 5785
 5790
 5795
 5800
 5805
 5810
 5815
 5820
 5825
 5830
 5835
 5840
 5845
 5850
 5855
 5860
 5865
 5870
 5875
 5880
 5885
 5890
 5895
 5900
 5905
 5910
 5915
 5920
 5925
 5930
 5935
 5940
 5945
 5950
 5955
 5960
 5965
 5970
 5975
 5980
 5985
 5990
 5995
 6000
 6005
 6010
 6015
 6020
 6025
 6030
 6035
 6040
 6045
 6050
 6055
 6060
 6065
 6070
 6075
 6080
 6085
 6090
 6095
 6100
 6105
 6110
 6115
 6120
 6125
 6130
 6135
 6140
 6145
 6150
 6155
 6160
 6165
 6170
 6175
 6180
 6185
 6190
 6195
 6200
 6205
 6210
 6215
 6220
 6225
 6230
 6235
 6240
 6245
 6250
 6255
 6260
 6265
 6270
 6275
 6280
 6285
 6290
 6295
 6300
 6305
 6310
 6315
 6320
 6325
 6330
 6335
 6340
 6345
 6350
 6355
 6360
 6365
 6370
 6375
 6380
 6385
 6390
 6395
 6400
 6405
 6410
 6415
 6420
 6425
 6430
 6435
 6440
 6445
 6450
 6455
 6460
 6465
 6470
 6475
 6480
 6485
 6490
 6495
 6500
 6505
 6510
 6515
 6520
 6525
 6530
 6535
 6540
 6545
 6550
 6555
 6560
 6565
 6570
 6575
 6580
 6585
 6590
 6595
 6600
 6605
 6610
 6615
 6620
 6625
 6630
 6635
 6640
 6645
 6650
 6655
 6660
 6665
 6670
 6675
 6680
 6685
 6690
 6695
 6700
 6705
 6710
 6715
 6720
 6725
 6730
 6735
 6740
 6745
 6750
 6755
 6760
 6765
 6770
 6775
 6780
 6785
 6790
 6795
 6800
 6805
 6810
 6815
 6820
 6825
 6830
 6835
 6840
 6845
 6850
 6855
 6860
 6865
 6870
 6875
 6880
 6885
 6890
 6895
 6900
 6905
 6910
 6915
 6920
 6925
 6930
 6935
 6940
 694

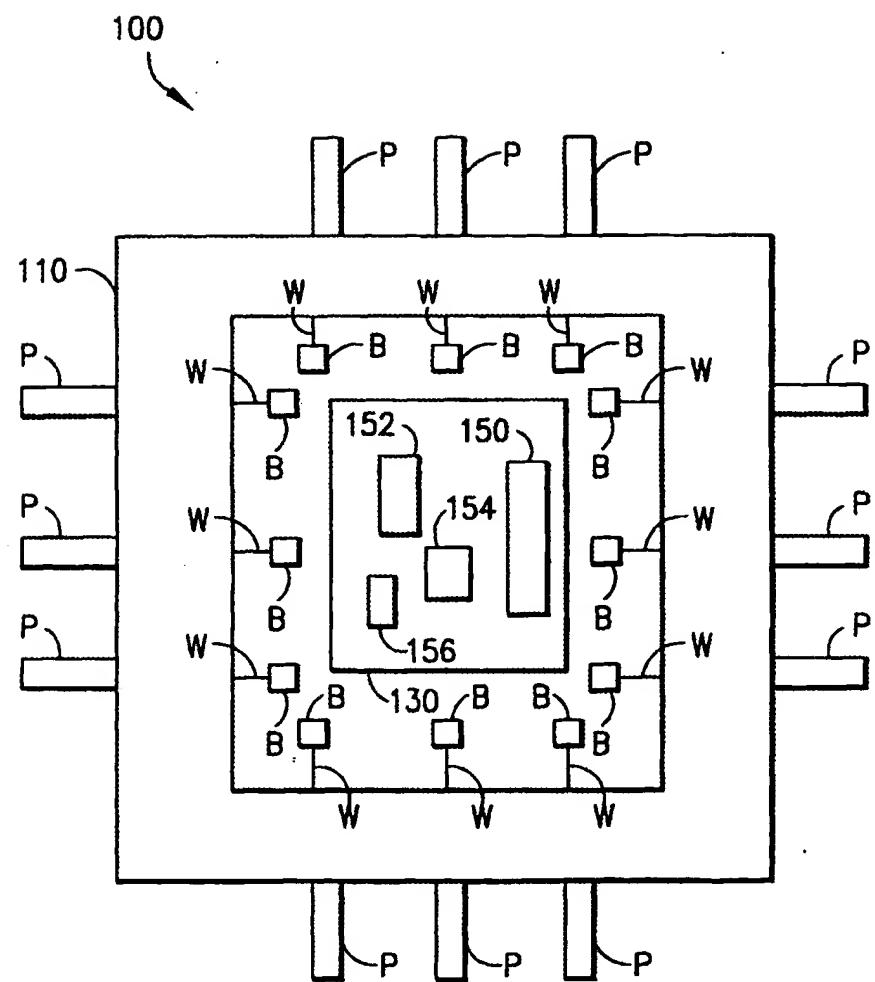


FIG.1

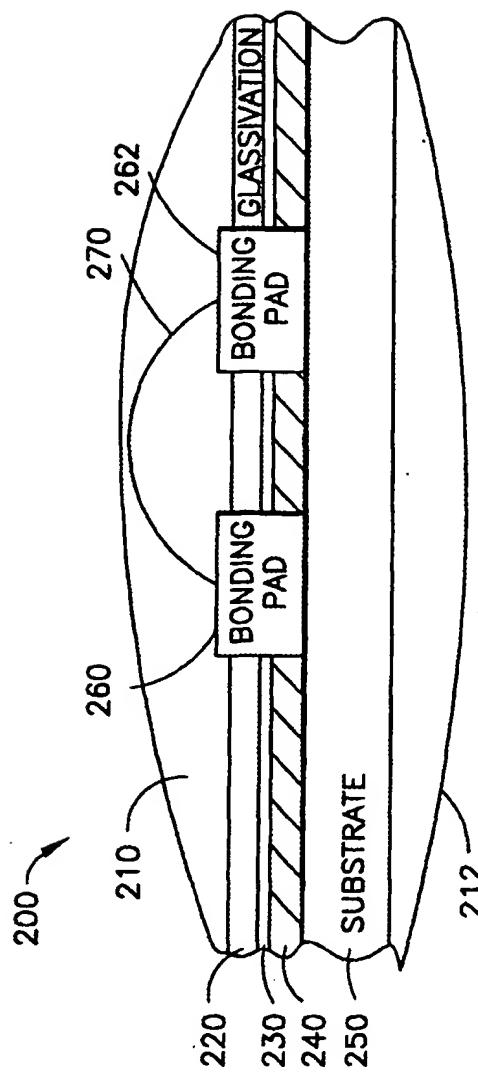


FIG.2

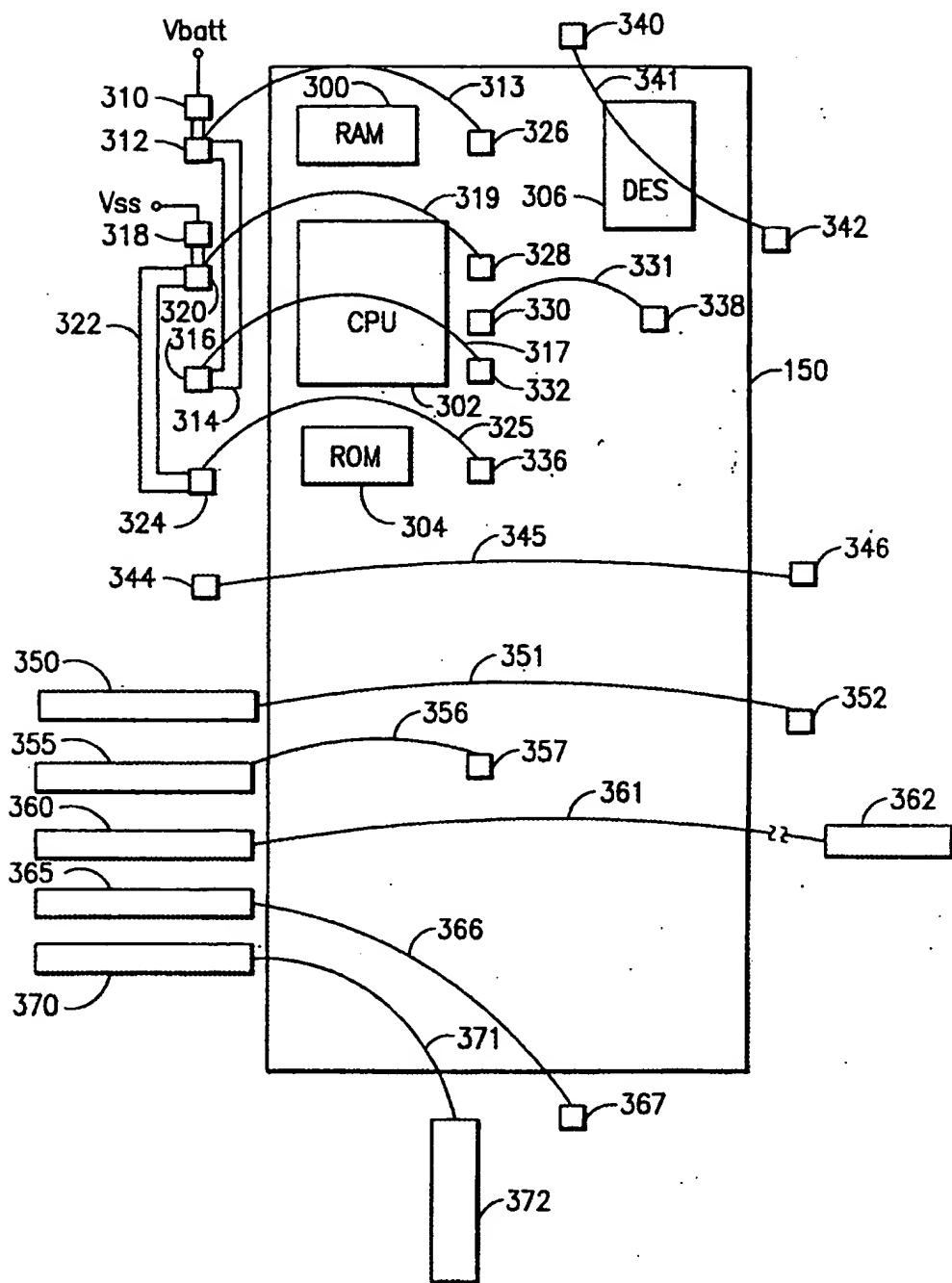


FIG.3

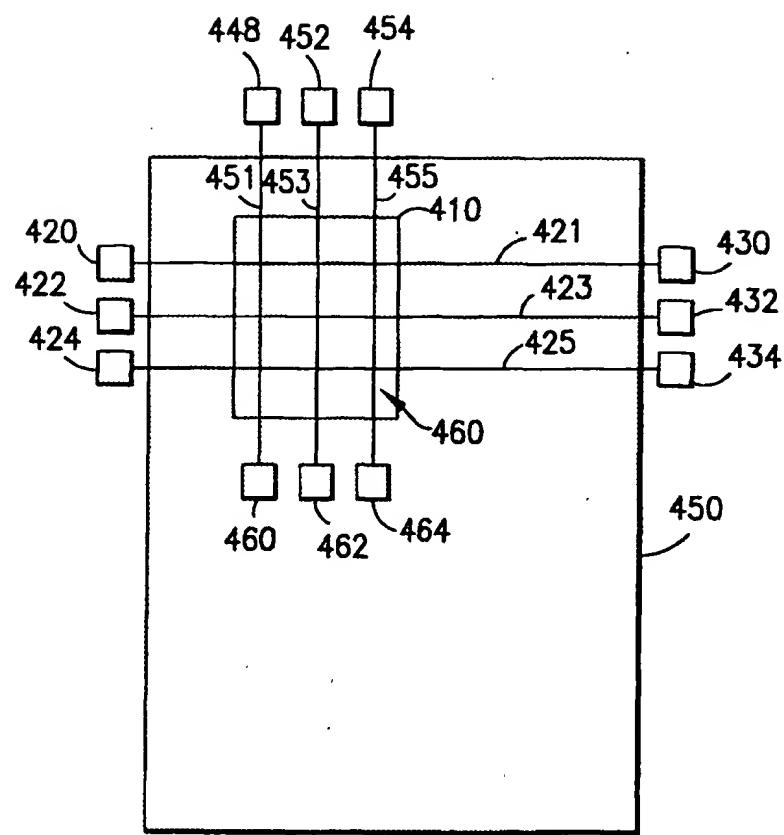


FIG.4